



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,176	08/28/2001	Danny M. Nessett	3COM-3716.TDC.US.P	6999

7590 01/05/2005

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER

HO, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/942,176

Applicant(s)

NESSETT, DANNY M.

Examiner

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 28 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-25 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1 recites the limitation "third value" in claim 1. There is insufficient antecedent basis for this limitation in the claim.

For the purposes of examination and from the specification stated by applicant, the Examiner shall take the "third value" to be a third nonce or value generated or supplied from within the access point server.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over (Menezes et al., Handbook of Applied Cryptography) in view of (Schneier, Applied Cryptography) and Lincke et al., US patent 6253326.

For the purposes of the rejection below and in accordance with standard cryptographic naming convention, Party has been called Alice, Party B, Bob, and Party T, Trent.

In reference to claim 1:

(Menezes et al., , pgs. 503-504 Sections on Otway-Rees protocol, Handbook of Applied Cryptography) discloses in a network access point, a method of processing encrypted communication, according to an encryption/decryption process, said method comprising:

- Receiving a first message from a wireless client, said first message comprising first values for a first random number and information identifying said wireless client and said access point and a first message authentication code of said information in said first message signed using a first signing key,
 - where the first wireless client is Alice, the first random number is the Nonce A, information identifying the client is her name, information identifying the access point is Bob, the message authentication code is an index number, and the message is signed message is the encryption by the key she shares with Trent, and this message is received by Bob.
- Generating a second message comprising second values for a second random number and information identifying said access point and said wireless client and a second message authentication code of said information in said second message signed using a second signing key.

- Where the second message is generated by Bob, the second random number is Nonce B, information identifying the access point is Bob's Name, information identifying the wireless client is Alice's name, the second message authentication code is an index number, and the message is signed or encrypted using another key, the one Bob shares with Trent.
- Sending said first values and said second values to an access point server, wherein said access point server generates a session key using said first and second values and third values provided by said access point server, such that said processing is shared by said access point and said access point server.
 - Where the message generated by Bob and Alice, are eventually both sent to Trent, the Access point server, where the first value is the random number of Alice, the second value is the random number of Bob. The session key is the session key generated by Trent, and the processing and decryption is shared between Bob and Trent.

Menezes et al. however fails to explicitly disclose using the first and second Nonce and generating a third value to be used in the generation of the session key. Menezes et al. also fails to explicitly disclose the hardware embodiment where Alice is a Wireless client, Bob is the Access point, and Trent is the Access Point server.

Key generation may employ any number of values. Schneier (p. 175, "X9.17 key generation") for example discloses X9.17 key generation which uses three different seeds for the generation

of a key. Schneier (p. 175, "X9.17 key generation", Applied Cryptography) further discloses that this method does not generate easy to remember keys, making it suitable for session keys.

Lincke et al. (Figure 4) discloses the use of a wireless client communicating with an access point, which then in turn communicates with a server. This setup appears to be common in wireless technology as a standard wireless topology. Additionally, Menezes et al. describes Alice, Bob, and Trent, as parties A, B, and T, suggesting that any digital processing device may be used to implement them and that only their respective interactions are important.

It would have been obvious to one of ordinary skill in the art to implement Alice, Bob, and Trent as the wireless client, wireless access point, and server, and to use they X9.17 key generation process to generate keys appropriate for use as session keys and to provide the benefits of the Otway-Rees algorithm in a wireless context.

In reference to claim 2:

(Menezes et al., , pgs. 503-504 Sections on Otway-Rees protocol, Handbook of Applied Cryptography) discloses receiving a third message conveying said session key from said access point server, said third message having a first portion and a second portion and verifying said second portion of said third message against said second values, where the third message is the message generated by Trent or party T which includes the new session key k which has a first and second portion for party A and party B, and the whole is transmitted to Party B, Bob. Bob

Art Unit: 2134

then verifies the second portion of the message against the second values in decrypting the second part of the message (12.29, 4(d)) and seeing if the second Nonce matches.

In reference to claim 3:

(Menezes et al., , pgs. 503-504 Sections on Otway-Rees protocol, Handbook of Applied Cryptography) discloses the method as recited in claim 1 further comprising:

Sending said first portion of said third message to said wireless client, wherein said wireless client verifies said first portion of said third message against said first value, such that said session key is shared between said wireless client and said access point and said access point server., where the first part of the message is passed to party A (12.29, 4(d)), where party A, the wireless client verifies by decrypting the message and checking if the original nonce matches.

In reference to claim 4:

(Menezes et al., , pgs. 503-504 Sections on Otway-Rees protocol, Handbook of Applied Cryptography) discloses the message as recited in claim 2 wherein said first portion of said third message further comprises data for ensuring validity of said first portion and wherein said second portion of said third message further comprises data for ensuring validity of said portion, where the first portion of the third message comprises the Nonce A for ensuring validity to the first party, and the second portion of the third message comprises Nonce B for ensuring validity to the second party. These values are the random values in claim 1, and as stated by the Applicant in specification, known in the art as Nonces.

In reference to claim 5:

The combination as rendered above in claim 1 discloses a method wherein said third value is correct for said encryption/decryption process, where the third value is used as a seed to a key generation, or an encryption process.

In reference to claim 6:

Lincke et al. (Figure 4) discloses the method as recited in claim 1 wherein said network is a wireless network.

In reference to claim 7:

(Menezes et al., , pgs. 503-504 Sections on Otway-Rees protocol, Handbook of Applied Cryptography) discloses the method as recited in claim 1 wherein said encrypting/decrypting process comprises a distributed symmetric key distribution process.

In reference to claim 8:

(Menezes et al., , pgs. 503-504 Sections on Otway-Rees protocol, Handbook of Applied Cryptography) discloses the method as recited in claim 7 wherein said distributed symmetric key process is Otway-Rees key cryptography.

In reference to claim 21:

Lincke et al. (Figure 4) discloses the computer usable medium of claim 17 wherein said computer system is an access point in a network.

Claims 9 – 16 are substantially similar to claims 1-8 and are rejected for the same reasons respectively.

Claims 17-20 are substantially similar to claims 1-4 and are rejected for the same reasons respectively.

Claims 22-25 are substantially similar to claims 5-8 and are rejected for the same reasons respectively.

Conclusion

5. The following prior art not relied upon is made of record.

(Schneier, pgs 59-60, Applied Cryptography) discloses a simplified version of the Otway-Rees algorithm.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (571)272-3838. The fax phone numbers for the

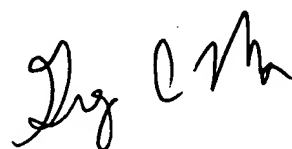
Art Unit: 2134

organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

December 15th, 2004

TMH

A handwritten signature in black ink, appearing to read "Greg C. Morse", is written in a cursive style.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100